Clean Copy
Sub. Specification

Method of securing a mobile telephone identifier and corresponding mobile telephone

This disclosure is based upon French Application No. 03/15078 filed December 19, 2003 and International Application No. PCT/EP2004/053469, filed December 14, 2004, the contents of which are incorporated herein by reference.

BACKGROUND OF THE INVENTION

The invention relates to mobile telephone handsets and, more particularly, to techniques that aim to reduce the possibilities of reusing a stolen handset.

Theft of mobile telephone handsets has become a real social problem. This has entailed a massive increase of violent theft cases in public places in recent years, due to the theft of such handsets. It has

been estimated, for example, that more than 150,000 mobile phones were stolen in 2001 in France alone. With a view to reducing this figure, the French authorities now demand that mobile telephone operators place an identifier of the stolen handsets on a black list. Every mobile handset has a unique identifier, called IMEI (International Mobile Equipment Identity), which is transmitted to the network used for communication. The IMEI of a handset reported as stolen is thus placed on a black list, which is already operational in France. When a handset included in the list attempts to establish communication, it can be blocked.

However, the IMEI is currently stored on a flash memory with poor security. In fact, there are software applications that allow a user to modify the IMEI of a handset, which are widely available on the internet. Therefore, as the European Commission has admitted, it is fairly easy to get around the creation of black lists of stolen handsets.

A technical recommendation by the ETSI proposes making it impossible to change the IMEI after the handset manufacturing process. This recommendation has been implemented mainly by recording the IMEI in a PROM, so that it cannot be physically modified.

This securitisation technique has certain drawbacks. Since the IMEI is read by the operating system of the handset, the use of a fraudulent operating system therefore makes it possible to modify the IMEI through the software in order to send the network a modified IMEI.

SUMMARY OF THE INVENTION

The invention aims to solve these disadvantages and therefore relates to a mobile telephone handset comprising:

- a storage support which is secured against fraudulent access, which stores the IMEI of the handset;
- a connector for a secure electronic module, which is associated with an operator;
- a handset operating system, which controls authentication of the IMEI storage support by a secure electronic module which is connected to the aforementioned connector in order to establish a secure communication channel between the storage support and the module and transmission of the IMEI over the secure channel to the secure electronic module.

According to a variant, the operating system controls the transmission of the IMEI to a mobile telephone operator by means of a secure OTA channel.

According to another variant, the handset comprises a secure electronic module associated with the operator connected to the connector. According to a further variant, the secure electronic module is a UICC.

It is also possible for the operating system to control authentication of the secure module by the storage support.

According to a variant, the secure electronic module and the storage support store encryption keys

that are adapted to securing the secure communication channel.

According to another variant, the secure module blocks the use of the handset when a false IMEI is detected.

The invention also relates to a method of securing the IMEI of a mobile telephone handset comprising the following steps:

- authenticating a secure storage support by memorising its IMEI by means of a secure electronic module associated with the operator and inserted in a connector of the handset, in order to establish a secure channel between the storage support and the secure module;

- transmitting the IMEI from the storage support to the secure module over the secure channel.

According to a variant, the secure module also transmits the IMEI to a mobile telephone operator over a secure OTA channel.

According to a further variant, the operator compares the IMEI with a black list of stolen handsets, and blocks the communications of the handset when the handset appears on the black list.

According to another variant, the secure module blocks the use of the handset when a false IMEI is detected.

BRIEF DESCRIPTION OF THE DRAWINGS

Further special features and advantages of the invention will appear clearly from reading the

description provided as a non-exhaustive example in relation to the appended drawings, in which:

- figure 1 shows the elements implemented according to one variant of the invention;
- figure 2 shows a diagram that illustrates the exchanges and steps performed by the elements according to one variant of the invention.

The invention suggests using a secure channel to perform the authentication of a storage support (secured against fraudulent access and containing the IMEI in its memory) by means of a secure electronic module associated with the operator and connected to the mobile handset. Such a secure electronic module is typically presented in the form of a UICC (Universal Integrated Circuit Card), for example as a SIM card. The IMEI is only transmitted to the secure channel when the IMEI's storage support has been authenticated.

DETAILED DESCRIPTION

Figure 1 thus shows a mobile telephone handset 1 according to the invention. The handset 1 comprises a storage support 2 secured against fraudulent access. This storage support 2 stores the IMEI 21 of the handset 1. The handset 1 also comprises a connector 3 for a secure electronic module such as a UICC 31. A secure communication channel 6 is established between the secure electronic module 31 connected to the connector 3 and the secure storage support 2. The secure communication channel 6 means that at least the secure module authenticates the storage support 2 using

any suitable means and guarantees the integrity and the confidentiality of all the data exchanged. A handset operating system 4 controls the authentication of the IMEI 21 storage support 2 by the secure module 31 connected to the connector (identified as step 101 in figure 2), and controls the transmission of the IMEI over the secure channel 6 to this secure module 31 (identified as step 102 in figure 2).

The IMEI is thus secured against dynamic modifications during its transmission over the communication channel 6. The IMEI received by the module 31 can therefore be considered to have been authenticated since it comes from the authenticated storage support 2 and was transmitted over the secure communication channel 6.

Obviously, if the authentication of the storage support 2 of the IMEI by the secure electronic module 31 signals an error, this electronic module 31 can take any measures required to point out this error and prevent the handset from being used.

It is therefore possible to block the handset without requiring communication with the operator's network. The operator can, in particular, avoid having to manage the keys or certificates that are associated with a handset. Such a block is therefore easier to implement. The telephone can also be blocked in this way without requiring any modifications of the operator networks: the infrastructures and protocols of the existing network can thus be conserved.

The storage support 2 secured against fraudulent access can be of a known type, for example a PROM. The static integrity of the information it contains is thus guaranteed.

In order to secure the channel 6 and to perform any necessary authentications between the storage support 2 and the module 31, the support 2 and/or the module can store encryption keys adapted to the desired type of encryption or authentication. The types of encryption or authentication to be used are already known. It is possible, in particular, to consider using session keys or static keys.

The integrity of the IMEI can be protected by a cryptographic calculation, which will be sent over the secure channel 6 to the secure module 31.

The operating system 4 can be memorised in a ROM memory and executed by a microcontroller. The operating system 4 will preferably establish a secure channel between the support 2 and the secure module 31 at the time of switching on the telephone handset or prior to a call.

The operating system 4 can be configured so that the secure module 31 authenticates the handset and checks the integrity of the data transmitted to it. It is also possible to plan for the secure module 31 to be authenticated by the secure support 2 of the mobile 1 and also for it to check the integrity of the data transmitted to it.

It is also possible to provide cryptographic calculation means contained in the secure module 31.

Black lists should nevertheless continue to be used for taking blocking measures. The IMEI can, in particular, be transmitted from the secure module to the operator's network, possibly by using a secure channel between the secure module 31 and the operator or in order to compare the authenticated IMEI with a black list and possibly to obtain a command from the network to block the handset. In the example of figure 2, the IMEI is transmitted to a server 7 in step 103. The server determines whether this IMEI is present in its black list. In step 104, the server transmits to the handset an indication of whether or not the IMEI is in the list. An indication of whether or not the IMEI is in the list can correspond to a command from the server to block the handset. The server can obviously take any other measure required to disrupt the fraudulent user. The server can, in particular, disconnect the handset from the operator's communication network or command the secure module to stop generating keys for the handset.

Several modes can be provided for transmitting the IMEI between the secure module and the operator's network.

This transmission can be carried out, in particular, by means of the operator's communication network, intended for transmitting communications between users. In the example of figure 1, the transmission is carried out between the handset and an operator 5 of a communication network.

The transmission is preferably carried out over a secure channel, in order to increase the level of security of the transmission. It is possible, in particular, to use the secure OTA channel originally intended for transmitting secure SMS messages and used mainly for transferring applets to the secure module.